COVERT CHANNEL USING POWER CONSUMPTION

Submitted by:

MRADU RATHORE

Supervisor:

DR PAOLO PALMIERI

Second Reader:

DR WHO

MSc Computing Science

School of Computer Science & Information Technology
University College, Cork

January 11, 2024

Abstract

This thesis investigates the feasibility of establishing a covert communication channel by modulating the power consumption of the Central Processing Unit (CPU). In an era where digital security is paramount, the development of unconventional data transmission methods has significant implications. Our research focuses on the deliberate manipulation of laptops' CPU power consumption, using this modulation as a means to covertly transmit information. This study is conducted through the lens of JavaScript programming, an option that demonstrates the ability to apply such techniques to commonly used high-level languages.

The methodology involves a two-step approach: first, a thorough analysis of CPU power consumption patterns under normal operating conditions, and second, implementation of modulation techniques to produce visible changes in power consumption. These fluctuations are used to encode binary data, effectively turning the CPU into a medium for secret communications. The study included extensive testing and analysis to compare the power consumption profiles of normal and modulated CPU states.

A major contribution of this thesis is the development of a novel JavaScript-based framework for CPU power modulation. This framework not only serves as a proof of concept for the feasibility of CPU-based covert channels, but also serves as a foundation for further research in this area. The findings of this research highlight the data transmission capabilities of such a channel as well as the challenges and limitations inherent in power-based modulation techniques.

This work opens new avenues for secure communications, especially in environments where traditional communication channels are monitored or restricted. It also raises important discussions regarding the detection and prevention of such covert channels, highlighting their potential use in both benign and malicious contexts. The thesis concludes with insights into future research directions, emphasizing the need for more sophisticated modulation techniques and the exploration of countermeasures to mitigate the security risks posed by such covert communication methods.

`uccthesis` class.

Declaration

I confirm that, except where indicated through the proper use of citations and references, this is my original work and that I have not submitted it for any other course or degree.

Signed: _____

Mradu Rathore
January 11, 2024

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In the current digital age, where the concepts of security and privacy are more important than ever, exploring innovative and unconventional methods for secure and discreet communication has become a focal point of interest in the field of cyber security. This thesis introduces a pioneering approach to covert communications that is significantly different from traditional methods, by focusing on the modulation of CPU power consumption as a means of transmitting information. This innovative strategy takes advantage of the computer's central processing unit (CPU) - a component universally recognized as the heart of computing power, which has not been extensively explored in existing literature or practices.

The use of JavaScript, a language traditionally associated with web development, to implement this concept marks a significant departure from standard practices in systems-level programming. This choice not only demonstrates the flexibility and potential of JavaScript, but also makes the method more accessible to a wider range of developers and researchers, given the widespread use of the language. This study sheds in-depth light on a relatively untapped area of cybersecurity, opening up new possibilities and approaches to secure communications.

The approach presented in this work provides a viable solution for secure information transfer, especially in scenarios where traditional communication channels are either under surveillance or at risk of being compromised. The reliance on CPU power consumption modulation offers an option that is less likely to be detected by standard network monitoring tools, thus adding an additional layer of protection. The primary objective of this research is to demonstrate the feasibility of creating a covert channel through CPU power modulation, exploring its practicality, efficiency and potential applications. This includes not only the technical aspects of implementing such a channel, but also an in-depth examination of its implications in the broader context of digital communications and security. Pushing the boundaries of traditional communication methods, this thesis contributes to the ongoing discourse on digital privacy and security, providing insights and paving the way for future innovations in the field.

`uccthesis` class, the main purpose of which is to write a thesis with minimal configuration.

1.1 Motivations

The motivation for this research arises from the growing need for secure and unobtrusive communication methods in a digital landscape dominated by sophisticated monitoring and surveillance systems. As digital interactions are increasingly scrutinized, the ability to transmit information in a way that avoids standard detection mechanisms is not only beneficial but often critical, especially in scenarios demanding high levels of privacy. This requirement increases further in environments where communication integrity and confidentiality are paramount, such as in government, defence, and some corporate sectors.

Traditional covert channels, although effective in some contexts, primarily rely on established network protocols or exploit software vulnerabilities. These methods, while simple, are becoming more vulnerable to advanced detection techniques as cybersecurity measures evolve. The strength of these traditional channels is constantly being challenged by advances in network monitoring technologies and the strength of security protocols. As a result, there is a growing motivation to seek alternative avenues for covert communications that are less dependent on traditional digital routes and thus more resistant to emerging surveillance technologies.

In this regard, CPUs emerge as a promising medium for covert communications. Ubiquitous in computing devices and at the heart of their operation, CPUs have characteristics that are often overlooked in the context of covert data transmission. One such feature is the power consumption pattern. One such feature is the power consumption pattern. While power consumption has been extensively studied for efficiency and thermal management, its potential for information transmission has not been adequately explored. This research addresses this gap by investigating the modulation of CPU power consumption as a novel covert communication channel.

Furthermore, the selection of JavaScript as the implementation tool significantly expands the scope and applicability of this research. The ubiquity of JavaScript in the world of software development, coupled with its evolving capabilities, provides a unique opportunity to implement CPU power modulation in a more accessible and versatile way, especially in server-side environments like Node.js. This approach not only demonstrates the ability of a high-level programming language to perform system-level operations, but also ensures that the techniques developed are within the reach of a vast range of developers and applicable on a wide variety of platforms are there.

In summary, this research is motivated by the aim of advancing a covert communication method that not only challenges the norms of existing technologies but also offers a new use of a fundamental computer component. By taking advantage of the unknown potential of CPU power patterns and combining it with the versatility of JavaScript, this study aims to contribute a unique and less traceable approach to the repository of secure communication technologies. The ambition is to expand the horizons of what is possible in the field of covert communications, paving the way for more secure and discreet methods of data transmission in an increasingly surveilled digital world.

1.2 Goals of This Work

The overarching goal of this research is to conceptualize, develop, and validate a new method of covert communication that takes advantage of modulation of CPU power consumption. This ambitious objective includes several key components and detailed steps, each of which contributes to the comprehensive understanding and practical application of this innovative approach.

Establishing a secret communication channel

The primary objective of this thesis is to establish a covert communication channel through modulation of CPU power consumption. This involves the development of a sophisticated method that allows precise control over the power usage patterns of the CPU. The challenge is to create a system that can produce visible changes in power consumption, which can then be used to secretly encode and transmit information.

Developing a Prototype System Using JavaScript

A main objective is to design and implement a prototype system capable of implementing the proposed power modulation technique. The system will be developed using JavaScript, chosen for its versatility and wide use. The prototype must be able to encode data across power consumption variations and decode this information at the receiving end, effectively demonstrating the practical application of CPU power modulation as a communication method.

Analyzing Effectiveness, Efficiency and Privacy

An essential goal is to comprehensively analyze the effectiveness, efficiency and privacy of the created communication channel. This includes evaluating the accuracy of data transmission (effectiveness), the rate of data transfer relative to power usage (efficiency), and the ability to remain undetected by standard monitoring devices (stealth). This analysis will help assess the feasibility and reliability of the covert channel in different operational environments.

Rigorous testing and evaluation

It is important to conduct thorough testing and evaluation to understand the capabilities and limitations of the covert channel. This involves simulating diverse operating scenarios to test system performance under different conditions, such as varying workloads and power conditions. The purpose of the testing phase is to identify and quantify error rates, data transmission speeds, and detection probabilities.

Contribution in the field of cyber security

In conclusion, this thesis seeks to make a significant contribution to the field of cybersecurity. By discovering and documenting an innovative method of secure communications, the research aims to advance knowledge in the field of covert channels. It will also evaluate the potential applications and implications of this technology, considering both its benefits in secure communications and its risks when employed for malicious purposes. The insights gained are expected to inspire future research and development in secure communications technologies and cybersecurity protections.

Chapter 2

Backgroung and Literature Review

This thesis's literature review section will conduct a thorough analysis of recent advancements and research in the subject of covert communication, with an emphasis on the utilisation of CPU power consumption as a medium.

2.1 Introduction to Covert Channels

Overview

Covert channels are communication methods used to transfer information covertly, usually in environments where direct or open communication is monitored or restricted. In the context of secure communications, covert channels are employed to bypass standard identification mechanisms, thereby ensuring the confidentiality and privacy of transmitted data. These channels are not part of designed communication routes and are often created by exploiting unintended functionalities or side effects of the system.

Historical Context

The concept of covert channels has evolved significantly over time. Historically associated with espionage and secret messaging techniques, these channels have found new life in the digital age. Initially, covert communication involved simple methods such as hidden ink or microdots. With the advent of computers and the Internet, the focus shifted to digital mediums. Covert channels in digital systems include exploiting network protocols, manipulating file metadata, or using hardware-based emissions (such as electromagnetic or thermal emissions) for data transmission. The evolution from physical to digital has greatly increased the scope and complexity of covert channels, making them an important topic in the field of cybersecurity.

Year	Development	Impact
Early 20th century	Microdots and concealed inks are used in espionage	Base for hidden communications; extensively employed in military and espionage missions
1940s	Cryptography emerged in World War II	Change to encrypted communications; heightened intricacy and safety in covert communications
1970s	Recognising covert channels in computer systems	Digital mediums of identification for covert communications
1980s	Exploitation of network protocols is on the rise	Growth of digital covert channels within computer networks
2000s	Using emissions from hardware such as electromagnetic	Hardware-based covert channel being introduced in computing devices
2010s	Emergence of complex software-based techniques	Enhanced complexity and efficacy of digital covert channels
2020s	Exploration of CPU based power modulation	A new strategy for covert communications that makes use of hardware attributes

Table 2.1: Timeline of Covert Channel Development
This table summarises significant advancements in covert channel history, ranging from conventional espionage methods to cutting-edge digital applications.

2.2 CPU's Power Consumption as Communication Channel

CPU Power Dyanamics

A CPU's power consumption is the result of a complex interplay of factors that are firmly based in computer architecture and electronic engineering principles. The fundamental factors that determine a CPU's power consumption are its operational state, which includes its clock speed, voltage, and type of operations performed. Power consumption is greatly impacted by variables such as transistor count, manufacturing method (7nm, 10nm technology, etc.), and workload type (CPU-intensive vs. idle state). The dynamic nature of these components complicates power consumption patterns, particularly in contemporary multi-core CPUs with sophisticated power management technologies like AMD's Precision Boost and Intel's Turbo Boost.

Possibilities for Covert Channel

The fluctuating nature of CPU power usage offers a fascinating way to communicate covertly. Information can be encoded by modulating power usage, which is simply generating a pattern or sequence of high and low power levels. Clock speed adjustments, CPU task intensity variations, or switching between power-efficient and power-intensive operations can all be used to achieve this modulation. In essence, the CPU would become a covert signal transmitter by interpreting the encoded data through the analysis of power consumption patterns. This is a stealthy technique to covert transmission because it uses a medium that is typically not checked for data leaks, which accounts for its subtlety.

2.3 Review of Existing Covert Communication Techniques

In this section we will delve deeper into the current scenario of covert communication methods. This exploration will include an in-depth analysis of both host-based and network-based covert channels, each with its own unique mechanisms and applications. We'll delve deeper into the intricacies of host-based channels, exploring how storage and time channels can be used within the same system for covert communications. Particular attention will be paid to the methods and nuances of network-based covert channels, where data is transmitted by manipulating network protocols or using time variations in network traffic. Additionally, we will expand our exploration to physical covert channels, including electromagnetic, electrical, thermal, acoustic, and optical channels, each of which presents unique advantages and challenges in the context of covert communications.

This comprehensive review will not only outline the technical mechanisms and

Factor	Description	Impact on Power	Relevance to Covert Communication
Clock Speed	The CPU's operating speed.	Speed increases result in higher power consumption	Rapid modulation may be possible at faster speeds, although detectability may also rise.
Voltage Level	The CPU's operating speed	Power consumption rises with voltage.	Modulation without a major influence on performance can be achieved by varying the voltage.
Workload Type	Task characteristics (such as computational intensity).	Power consumption rises with intensive tasks.	A pattern of power usage for data encoding can be created using several tasks.
Manufacturing Process	The technology that goes into making CPUs.	Power efficiency is typically increased by more sophisticated procedures.	More sophisticated procedures could enable more precise control of power modulation.
Transistor Count	The quantity of transistors within the central processing unit.	Increased counts may result in higher power consumption.	Influences modulation potential and power control granularity.
Power Management Features	Features such as Turbo Boost from Intel.	Can dynamically modify power consumption.	Covert communication techniques may need to take advantage of these capabilities or take them into consideration.

Table 2.2: Factors Affecting CPU Power Consumption
This table offers a foundation for comprehending how different features of CPU operation and design can be used, or must be taken into account, while creating a technique for covert communication using modulation of power usage.

practical applications of each type of covert channel but also discuss their detection difficulties and countermeasures. By doing so, we aim to present a complete picture of the current state-of-the-art in covert communication, thereby setting the stage for our exploration into CPU power consumption as a new medium for covert communication. This section will provide the necessary background and contextual understanding, allowing us to situate our research within the broader landscape of covert communications technologies and highlight the contribution of our work to this area.

2.3.1 Network-Based Channels

Network-based covert channels have become a major part of the cybersecurity landscape. These channels use network protocols and communications to transmit data anonymously. Common methods include manipulating packet headers, increasing the time interval between packets, or using unused or less monitored protocol fields. These technologies can effectively transmit data across network boundaries, often bypassing standard security measures such as firewalls and network monitors. However, their effectiveness is dependent on the depth of network inspection and the sophistication of network security systems.

Types of Network-Based Covert Channels

- **Protocol manipulation covert channels** represent a sophisticated method in the realm of network-based covert communications. These channels operate by subtly altering or exploiting standard features and fields of network protocols to transmit data that is not easily detectable. The essence of this technology lies in the ability to use protocols designed for data transmission in such a way that they are usually not monitored, allowing information to be stolen through regular communication routes without arousing suspicion. Implementation of protocol manipulation can vary, but typically involves careful alteration of protocol header fields or payloads. For example, in TCP/IP communications, some fields in the packet header, such as sequence or acknowledgment number, may be slightly modified to carry secret information. Even fields designated as 'reserved' or 'unused' in various protocols provide the opportunity to embed data without affecting the standard functioning of the packet. This manipulation must be subtle enough to avoid disrupting the normal operation of the network and to avoid detection by network monitoring systems. The challenge is to maintain protocol compliance; The modified packets must still conform to the expected structure of legitimate traffic. Additionally, these covert channels are often bandwidth-limited, as only small amounts of data can be embedded in these areas without raising red flags. On the detection and defense front, uncovering these covert channels requires sophisticated network monitoring tools equipped with Deep Packet Inspection (DPI). DPI can analyze packet headers and payloads in detail, searching for anomalies or patterns that deviate from standard protocol behavior. However, the efficacy of DPI in detecting such manipulation depends largely on the subtlety

and cleverness of the covert channel design. Additionally, statistical analysis of network traffic can be employed to detect irregularities or consistent patterns that may indicate the presence of a covert channel. Defenses against protocol manipulation often include stringent network traffic normalization or sanitization, where packets are systematically inspected and any non-standard modifications are cleaned up at network gateways or critical points. Despite these measures, the inherent complexity and ubiquity of network protocols continues to make protocol manipulation a powerful and elusive tool in covert communications.

- **Timing analysis in the context of covert channels** is a method that relies on the timing of certain events or operations to convey information. This type of covert channel can be implemented in both host-based and network based environments. In host-based systems, timing analysis may involve measuring the time it takes for the system to respond to certain requests or perform specific operations. In network based systems, this often revolves around the time interval between data packets sent over the network. The basic concept is to encode data in the time domain the duration of a signal, the interval between signals, or the specific time pattern of a sequence of events.

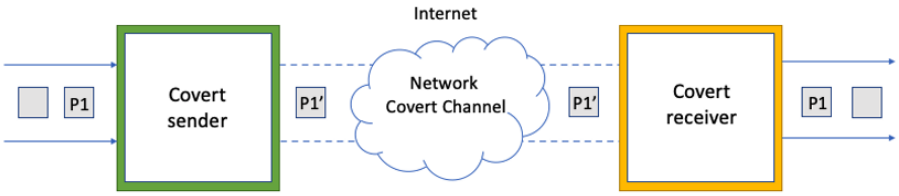

Figure 2.1: An example of how to use a network covert channel.

2.3.2 Hardware-Based Covert Channels

Hardware-based covert channels represent a unique and often sophisticated method of covert communication that takes advantage of the physical or operational characteristics of computer hardware. Unlike network or host-based channels, which rely on manipulation of data or network packets, hardware-based channels exploit physical phenomena associated with the operation of hardware components. These channels are diverse, spanning various aspects such as electromagnetic emissions, power fluctuations, thermal emissions, acoustic signals, and optical manipulation.

Types of Hardware-based Covert Channels

- **Electromagnetic emissions:** This type of covert channel uses electromagnetic waves naturally emitted by electronic devices during normal operation. By modulating these emissions, data can be transmitted to a receiver equipped with the required sensors. The primary challenge here is the need for specialized equipment to both transmit and receive the modulated signals, as well as the need for proximity to the emitting device.

- **Power fluctuation channels**, as a subgroup of hardware-based covert channels, exploit variations in the power consumption patterns of electronic devices to transmit secret information. This technology is particularly interesting because power use, which is a fundamental characteristic of any electronic operation, usually goes unnoticed in routine security monitoring. The main principle involves modulating the power draw of a device such as a CPU or GPU in a controlled pattern. These patterns can encode data, effectively turning fluctuations in power usage into a secret communication medium. Encoded messages are extracted by analyzing variations in power consumption over time. Such modulation can be achieved in a variety of ways, such as alternating between high and low computational tasks or adjusting operational parameters that directly affect power usage.

  The covert nature of power fluctuation channels makes them uniquely advantageous in scenarios where traditional communications channels are either heavily monitored or impractical. Unlike electromagnetic or acoustic emissions, which require physical proximity and special detection equipment, power fluctuations can be more discreet with less risk of interception. However, this precision comes with its challenges. Implementing an effective power fluctuation covert channel requires precise control over the device's power conditions. Furthermore, the encoding and decoding mechanisms must be sophisticated enough to distinguish intentional modulation from normal variations in power usage due to standard device operation. Additionally, external factors such as varying power supply conditions or other environmental influences may affect the reliability of these channels. Despite these challenges, exploring electrical fluctuations as a means of covert communication is attractive, especially in the context of growing interest in low-profile, non-traditional data transmission methods in the field of cybersecurity.

- **Thermal Emissions:** In this case, data is transferred by the heat produced by electrical equipment. It is possible to send information discreetly by employing thermal sensors and modifying the thermal output, such as the heat generated by a CPU. The problem with thermal emissions is the influence of temperature variations in the surrounding environment as well as the requirement for close proximity.

- **Acoustic Channels:** These channels make use of vibrations or sounds that hard-

ware parts, like fans or hard drives, create. Data can be sent discreetly by modifying these sonic emissions at frequencies that are normally undetectable to the human ear but detected by specialised equipment. The main issues facing these channels are ambient noise and the requirement for a quiet working environment.

- **Optical Channels:** LEDs and other components that emit visible or infrared light can be used to create optical covert channels. By varying the light's frequency or intensity, data can be communicated. These channels are easier to intercept than other hardware-based techniques, but they do require a direct line of sight or close proximity between the transmitter and receiver.

2.3.3 Host-based covert channels

Host-based covert channels are methods of communication that occur within the same computer system, exploiting various features and components of the host to bypass security mechanisms and transmit information in a way that was intended by the system's designers. Not intended. These channels can be particularly challenging to detect because they operate within the scope of a single system, often using legitimate functionalities in unexpected ways.

Types of Host-Based Covert Channels

- **File System Covert Channels** uses covert communication method that exploits the computer's file system to transmit information secretly. These channels take advantage of various aspects of the file system, such as file attributes, metadata, or space allocated to files. For example, an application may subtly alter a file's timestamp or permissions to encode the data, each modification representing a fragment of the secret message. Another common technique involves using file slack space, which is unused space at the end of a file cluster. Hidden data in Slack spaces is often ignored because it does not affect the normal operation or size of the file. Additionally, steganography can be employed, where data is hidden within a file in such a way that it appears normal and unchanged to an unsuspecting observer. For example, this may involve embedding secret messages within image or audio files. Detecting and mitigating file system covert channels requires careful monitoring of file system access patterns, regular analysis of file contents for irregularities, and the use of file integrity monitoring tools to track any unauthorized changes to files. These channels are particularly challenging to identify because they use legitimate system functionalities for covert communications, often leaving minimal traces.

- **Process-based covert channels** refer to covert communication methods that exploit the operation and interactions of processes within a computer system. These channels take advantage of the shared resources and inter-process communication mechanisms that are inherent in modern operating systems. For

example, a process can control its consumption of system resources such as CPU time or memory usage in a specific pattern. Another process, given these usage patterns, may decode the information being transmitted. This type of covert channel may also involve subtle manipulation of process conditions or synchronization events. For example, process execution timing, thread scheduling, or semaphore signals can be used to communicate hidden messages. These channels are particularly lethal because they take advantage of normal system functions in unexpected ways, making detection challenging. To counter process-based covert channels, system administrators and security software must monitor unusual process behavior and unexplained resource usage patterns. Enforcing strict access controls and separating processes with different privilege levels can also help reduce the risk of such covert communications. However, it is difficult to completely eliminate these channels due to the complexity and dynamic nature of process interactions in modern computing environments.

- **Registry-based covert channels** are a unique form of covert communication found primarily in systems that use the registry for configuration and settings, such as Microsoft Windows. These channels exploit the registry's ability to store data, using it as a medium to covertly transfer information between processes or entities. Malicious software or users can encode data in registry keys modifying, adding, or rearranging them to convey the information they want. This data can be decoded by a user knowing another process or encoding scheme. For example, the presence or absence of certain keys, the order of entries, or the values of specific settings can be manipulated to carry hidden messages. Detecting these covert channels includes monitoring registry access for unusual patterns and scanning for unexplained changes to the registry. However, since the registry is a legitimate and frequently used feature of the operating system, it can be challenging to distinguish between normal and covert modifications. The secret nature of these channels, combined with the registry's important role in system operation, makes them a particularly covert method of covert communication.

- **Network stack covert channels** exploit the complexities of network protocols and communications to transmit information anonymously. These channels manipulate various aspects of network packet formation and transmission, such as header fields, packet timing, or packet size, to encode and send secret messages. For example, a sender may subtly alter values in unused or optional header fields of a TCP/IP packet, or modify the timing of packet transmission to convey hidden information. The recipient, aware of the encoding scheme, can then extract this information by observing these subtle changes in network traffic. This type of covert channel is particularly challenging to detect because it conceals itself within legitimate network communications, allowing it to blend in with regular traffic. To counter these channels, deep packet inspection and sophisticated network monitoring tools are often required, capable of analyzing traffic patterns and identifying anomalies that may indicate covert communications. However,

the sheer volume and complexity of network traffic, as well as the need to avoid disrupting legitimate communications, makes managing network stack covert channels a demanding task in cybersecurity.

- **Peripheral device covert channels** use hardware devices connected to the computer, such as keyboards, printers, or even screens, to covertly transmit information. These channels can be very simple yet effective. For example, a piece of malware might manipulate the blinking pattern of the keyboard's LED lights (Caps Lock, Num Lock, etc.) to encode data. Alternatively, slight changes in screen brightness or noise emitted by the printer may contain hidden messages. These subtle manipulations are generally imperceptible to an average user but can be detected and decoded by an informed receiver with the right equipment. Because these peripheral devices are standard and essential components of computer systems, identifying and mitigating such covert channels can be challenging. It is important to monitor and restrict physical security measures as well as software controls on peripheral devices to reduce the risk of such covert communication methods. However, the diversity and ubiquity of peripheral devices, combined with their direct interaction with the physical world, makes peripheral device covert channels a unique and complex category in the field of cybersecurity.

- **Cache covert channels** take advantage of the CPU cache, a key component in modern computers, to facilitate covert communications. These channels operate by manipulating the access patterns to the cache memory. For example, a process may intentionally access specific memory locations to influence the state of the cache (such as causing a cache hit or miss). Another process can infer the transmitted information by observing the resulting changes in cache performance. This may involve measuring the time taken to access certain memory addresses, with variations indicating different bits of data. Since cache use is a fundamental and high-speed aspect of computer operation, these covert channels can be extremely fast and difficult to detect. They exploit the physical properties of the hardware, making them less dependent on specific software vulnerabilities. Detecting these channels requires sophisticated monitoring of anomalies in cache access patterns and system performance. However, the technical complexity and need to avoid disrupting legitimate cache operations make cache covert channels particularly challenging to mitigate within the scope of cybersecurity.

- **API covert channels** are a form of covert data transmission that manipulate the way applications interact with system APIs (application programming interfaces). These channels exploit the common functionality of APIs to encrypt and transmit information anonymously. For example, a program may vary the frequency, timing, or specific sequence of API calls to communicate hidden messages. The data is encoded in the pattern or nature of these calls, which any other process or entity aware of the encoding scheme can decode. This approach is particularly stealthy because it uses legitimate API functions, allowing secret communications to blend seamlessly with regular application activities. Detecting these channels

involves closely monitoring API usage patterns for anomalies or irregularities that deviate from standard application behavior. However, given the large number of API calls occurring in a system and their legitimate variability, identifying and mitigating API covert channels is a significant challenge in cybersecurity. Their effectiveness depends on the subtlety with which they use the standard operations of the software interface.

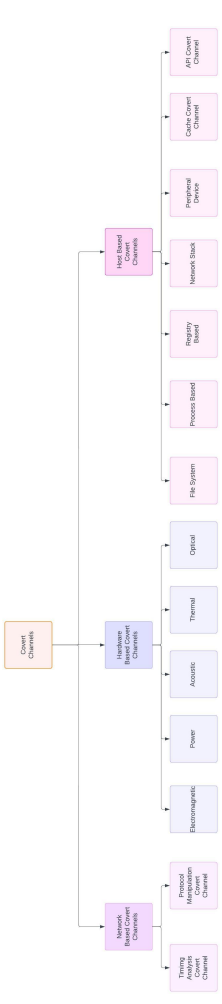

Figure 2.2: Types of Covert Channels

Chapter 3

Bugs and Requests for Features

Bugs and requests for features may be reported by email to `dongen@cs.ucc.ie`. When reporting bugs, please describe the bug as well as providing a *minimal* example.